MAGERIT
Versión 1.0

Metodología
de Análisis y Gestión de Riesgos
de los Sistemas de Información

Guía para responsables del
dominio protegible

1 INTRODUCCIÓN

1.1 Para quién y para qué esta Guía

Esta Guía se dirige a los Directivos de un Dominio funcional de la Organización cuya misión o cometido requiere sistemas de información y éstos seguridad de funcionamiento.

Los Directivos mencionados necesitan conocer de forma precisa los problemas que conlleva la falta de seguridad de los sistemas de información. Para tener idea de la importancia que han adquirido estos sistemas de información, basta con plantearse interna y sinceramente esta pregunta: ***¿Cuánto tiempo se puede mantener esa misión o cometido si deja de funcionar todo el sistema de información que ahora usa el departamento?*** La hipótesis afortunadamente es remota, pero no imposible, según se ve en todo tipo de ejemplos difundidos por la prensa: incendios de sedes centrales de bancos donde la pérdida más crítica es el sistema de información; errores de programas que paralizan las comunicaciones bancarias de medio país y con ellas todas las transacciones financieras; facilidades de acceso a redes de información reservada, cuyas violaciones de confidencialidad causarían graves perjuicios morales e incluso estratégicos ...

No cabe decir ya que éstos son accidentes excepcionales: también lo eran para los que los han soportado, hasta que han ocurrido. La seguridad no es una limitación a la tecnología, sino la condición básica para su empleo equilibrado y beneficioso. La necesidad de prevención no es nueva: por ejemplo nadie deja de viajar porque puede tener un accidente, pero se viaja más tranquilo con un seguro, aunque sólo evite algunas de sus consecuencias.

En ***circunstancias normales***, el logro del cometido de un departamento depende de una cooperación estrecha entre sus directivos y sus 'dirigidos' (ambos 'usuarios' de las técnicas informáticas), con los proveedores 'informáticos' de dichas técnicas. Para prever y dominar las ***circunstancias anormales***, esa cooperación debe extenderse e intensificarse al terreno de la seguridad, donde los directivos y los usuarios tienen un papel aún más imprescindible de corresponsabilidad que en circunstancias normales (ya que, en materia de seguridad las personas desempeñan papeles aún más relevantes que los de las técnicas).

La corresponsabilidad en materia de seguridad entre Directivos del Dominio'usuario' e informáticos tiene un marco preciso. La organización confía a los primeros la gestión de unos activos o recursos de los que son responsables ante ella, también en materia de la seguridad de los sistemas de información que utilizan. Esta Guía ayuda de forma sencilla a explicar el papel de los directivos como **'Responsables del Dominio'** protegible en esta corresponsabilidad, para que puedan asumirla lo más simple y eficazmente posible.

La legislación también empieza a plantear obligaciones cada vez más precisas en la materia: para el sector público el Real Decreto 263/1996 sobre técnicas electrónicas, informáticas y telemáticas; y de forma más extensa pero aún colateral la ampliamente conocida LORTAD, Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de Datos de carácter personal, en su artículo 9.

1.2 La Gestión de la seguridad y el método MAGERIT

La Gestión global de seguridad de los sistemas de información es una acción recurrente (es decir, se ha de reemprender periódicamente debido a los cambios de esos sistemas y de su entorno) que comprende dos grandes bloques:

- Un bloque está compuesto por varias Fases que se apoyan en técnicas generales adaptadas al campo de la seguridad. Unas 'preparan el terreno', como la determinación de sus objetivos, estrategia, política; planificación y organización específicas. Otras 'siembran y cosechan' la seguridad, como la implantación de salvaguardas y otras medidas, la concienciación de todos y la reacción a cada incidencia, manejándola, registrándola y recuperándola.

- El otro bloque está constituido por la fase de **Análisis y Gestión de Riesgos,** que es el núcleo de 'medición' y cálculo de la seguridad, con técnicas de proceso especiales (propias del ámbito de la seguridad). Para realizar este segundo bloque, el Consejo Superior de Informática ha elaborado MAGERIT, la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas, como respuesta a la dependencia creciente de éstas (y de toda la sociedad) de las Tecnologías de la Información y las Comunicaciones.

Para proporcionar la información sobre el primer bloque que necesita todo directivo 'usuario' de sistemas de información, el Ministerio de Administraciones Públicas y el Consejo Superior de Informática han editado la **'Guía de la Seguridad de los Sistemas de Información para Directivos de las AA.PP.',** preparada por el 'Grupo Ad-hoc 2' de Directrices de Seguridad de los Sistemas de Información del Comité del Consejo Superior de Informática de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales.

Como la Guía de Seguridad citada concentra en un solo apartado el bloque de Análisis y Gestión de Riesgos, se complementa con esta Guía para Responsables del Dominio protegible, que forma parte de las Guías MAGERIT y ofrece la información que necesitan los Directivos, considerados ahora en su corresponsabilidad sobre su Dominio en materia de seguridad. Así pueden cooperar estrechamente con el Analista de Riesgos que usa MAGERIT con el **objetivo** de investigar la seguridad de los sistemas de información de su Dominio y recomendar las salvaguardas o las medidas apropiadas que deberían adoptarse para promover y asegurar dicha seguridad.

2 ELEMENTOS DEL ANÁLISIS DE RIESGOS

En la realización de un Análisis y Gestión de Riesgos según MAGERIT, el Analista de Riesgos es el profesional especialista que maneja seis elementos básicos:

- Activos
- Amenazas
- Vulnerabilidades
- Impactos
- Riesgo
- Salvaguardas (Funciones, Servicios y Mecanismos)

Para poder identificar estos elementos en cada Dominio, es muy importante que el Responsable del Dominio protegible:

- conozca, transmita y valore los aspectos de la seguridad de los **Activos** de su Dominio;
- comprenda su **Vulnerabilidad** o sea la posibilidad de ataque de cada Amenaza (identificada en colaboración con el Analista de Riesgos).
- valore el **Impacto** consecuente al posible ataque sobre cada uno de sus Activos.

Esta Guía ayuda básicamente a clarificar estas tareas solicitadas al Responsable del Dominio protegible.

2.1 Identificación de los Activos protegibles del Dominio

*Los Activos son los **recursos** del **sistema de información o relacionados** con éste, necesarios para que la **organización funcione** correctamente y alcance los **objetivos** propuestos por la dirección.*

Como no tiene sentido hablar del sistema de información aislado desde el punto de vista del riesgo,

MAGERIT tiene en cuenta cinco grandes categorías de Activos:

1. El **entorno** o soporte del Sistema de Información, que comprende activos ***tangibles*** (como edificaciones, mobiliario, instalación física en los lugares de trabajo y según los casos, redes de información externas), ***equipamiento de suministro auxiliar*** (energía, climatización, comunicaciones) y ***personal*** (de dirección, operación, desarrollo, etc.)

2. El **sistema de información** propiamente dicho del Dominio (hardware, redes propias, software básico, aplicaciones, ...)

3. La propia **información** requerida, soportada o producida por el Sistema de Información que incluye los datos informatizados, entrantes y resultantes, así como su estructuración (formatos, códigos, claves de cifrado) y sus soportes (tratables informáticamente o no)

4. Las **funcionalidades del Dominio** que justifican al Sistema de Información, incluido desde el personal usuario a los **objetivos** propuestos por la **dirección del Dominio**.

5. **Otros Activos**, de naturaleza muy variada, por ejemplo la imagen de la organización, la confianza que inspire, el fondo de comercio, la intimidad de las personas, etc.

Estas 5 categorías de Activos se articulan como las 5 ‘capas’ principales en el diseño de la seguridad, desde el punto de vista de las repercusiones en ‘cadena’ de los problemas de seguridad de unos Activos sobre otros. Así, tomando un ejemplo real, un fallo en la red de conexión de datos (Activo de tipo **Entorno**) provoca la imposibilidad de alimentar el **Sistema de Información** (por ejemplo de una sucursal bancaria) que no obtiene así la Información de las cuentas de sus clientes, con lo que no puede ejercer las **funcionalidades de la organización** (atender a los clientes) y pierde imagen ante éstos (e incluso a ellos mismos) como ejemplo de esos **otros activos**.

La ‘cadena’ anterior de Activos constituye un recorrido de un ‘árbol de activos’ que arranca del activo ‘tronco’ (dónde se origina el primer fallo) y pasa a los activos relacionados de la siguiente capa (por las ramas troncales del árbol) y de éstos a los activos de las otras capas, hasta agotar éstas (por ramas, ramillas y hojas).

2.2 Valoración de Activos

Tras identificar los Activos de su Dominio a efectos de seguridad y los ‘árboles de activos’ que transmiten los fallos de unos a otros, el Responsable del Dominio protegible procura realizar al menos una de las formas de valoración (intrínseca o al menos del estado de seguridad) y registrarla como característica principal de cada Activo, para poder seguir desarrollando el Análisis y Gestión de

Riesgos.

El Activo puede tener dos formas clásicas de valoración, cualitativa y cuantitativa. La **valoración cualitativa** corresponde a **su *valor de uso*** y la **cuantitativa** a **su *valor de cambio*** (cuando éste tiene sentido para ciertos tipos de Activo).

Para realizar **la valoración de un Activo,**el Responsable del Dominio protegible se encuentra en estas situaciones:

- Toma directamente los valores de ciertos Activos que están ***inventariados***. MAGERIT recoge las clasificaciones y estructuración de los inventarios que corresponden a los Activos de las capas 1 (**Entorno**) y 2 (**Sistema de información**) a partir del Sistema IRIA de Información sobre Recursos Informáticos de las Administraciones Públicas preestablecido por el Consejo Superior de Informática y permite tomar fácilmente otros inventarios relacionados con la Contabilidad patrimonial.

- Puede ***inventariar*** otros Activos como Aplicaciones que cubran ciertas **funcionalidades del Dominio** (capa 3 de Activos) o la obtención de determinada **Información** (capa 3 de Activos), valorándolos por su coste de producción o de adquisición en el mercado.

Muchos Activos del Dominio en estudio **no son inventariables** en sentido contable o como **'valor de cambio'** (apto por ejemplo para reposición en caso de deterioro); pero no por ello dejan de tener **'valor de uso'** para la Organización (e incluso a veces un valor decisivo). El Responsable del Dominio protegible suele poder apreciar cualitativamente ese valor de uso por la carencia del Activo.

Esta apreciación de los Activos medida por su posible 'carencia' es evidentemente **cualitativa** y, a efectos de la seguridad, busca sólo una orientación para calibrar el posible **impacto** que la materialización de una amenaza puede provocar en el activo. Para evitar redundancias o contradicciones en valoraciones tan delicadas, la valoración de Activo se puede posponer hasta la valoración de sus Impactos, donde también se realizará la otra forma, también cualitativa, de **valoración del estado deseado de seguridad** de los Activos para sus 4 subestados (de autenticación, confidencialidad, integridad, disponibilidad)

2.3 Conocimiento de las Amenazas

Las amenazas se definen como los **eventos** que **pueden** desencadenar un incidente en la organización, produciendo daños **materiales** o pérdidas **inmateriales** en sus activos.

El Responsable del Dominio protegible tiene un papel de cooperante con el Analista de Riesgos en la identificación de las amenazas que pueden actuar sobre los activos de su Dominio. MAGERIT considera distintos 'productores' de las Amenazas (no humanos, humanos involuntarios o humanos voluntarios) para tener en cuenta la **diversidad de sus causas** , independientemente de sus consecuencias. Cada tipo de productores genera un tipo de causas de los cambios del estado de seguridad en los Activos: **accidentes, errores e intervenciones intencionales**, éstas realizadas con presencia del agresor bien **física** bien **por 'teleacción'** (usando medios de comunicación). Las Amenazas se clasifican así:

Grupo A de Accidentes

A1: **Accidente físico de origen industrial:** incendio, explosión, inundación por roturas, contaminación por industrias cercanas o emisiones radioeléctricas

A2: **Avería:** de origen físico o lógico, debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema

A3: **Accidente físico de origen natural:** riada, fenómeno sísmico o volcánico, meteoro, rayo, corrimiento de tierras, avalancha, derrumbe, ...

A4: **Interrupción de servicios o de suministros esenciales:** energía, agua, telecomunicación, fluidos y suministros diversos

A5: Accidentes mecánicos o electromagnéticos: choque, caída, cuerpo extraño, radiación, electrostática ...

Grupo E de Errores

E1: Errores de utilización ocurridos durante la recogida y transmisión de datos o en su explotación por el sistema

E2: Errores de diseño existentes desde los procesos de desarrollo del software (incluidos los de dimensionamiento, por la posible saturación)

E3: Errores de ruta, secuencia o entrega de la información en tránsito

E4: Inadecuación de monitorización, trazabilidad, registro del tráfico de información

Grupo P de Amenazas Intencionales Presenciales

P1: Acceso físico no autorizado con inutilización por destrucción o sustracción (de equipos, accesorios o infraestructura)

P2: Acceso lógico no autorizado con intercepción pasiva simple de la información

P3: Acceso lógico no autorizado con alteración o sustracción de la información en tránsito o de

configuración; es decir, reducción de la confidencialidad para obtener bienes o servicios aprovechables (programas, datos ...)

P4: Acceso lógico no autorizado con corrupción o destrucción de información en tránsito o de configuración: es decir, reducción de la integridad y/o disponibilidad del sistema sin provecho directo (sabotaje inmaterial, infección vírica..)

P5: Indisponibilidad de recursos, sean **humanos** (huelga, abandono, rotación) o **técnicos** (desvío del uso del sistema, bloqueo).

Grupo T de Amenazas Intencionales Teleactuadas

T1: Acceso lógico no autorizado con intercepción pasiva (para análisis de tráfico...)

T2: Acceso lógico no autorizado con corrupción o destrucción de información en tránsito o de configuración

T3: Acceso lógico no autorizado con modificación (Inserción, Repetición) **de información en tránsito**

T4: Suplantación de Origen (del emisor o reemisor, 'man in the middle') **o de Identidad**

T5: Repudio del Origen o de la Recepción de información en tránsito

2.4 Estimación de las Vulnerabilidades

La **Vulnerabilidad** de un Activo se define como la potencialidad o posibilidad de **ocurrencia** de la materialización de una Amenaza sobre dicho Activo.

La Vulnerabilidad es por tanto una **propiedad de la relación** entre un Activo y una Amenaza y se clasifica de acuerdo con éstos (conviene centrarse en las amenazas más fácilmente materializables y/o más impactantes sobre los Activos amenazados para evitar la inmanejable explosión combinatoria de todas las posibles amenazas sobre todos los activos retenibles). La estimación de la vulnerabilidad es una operación necesaria que sólo deben hacer buenos conocedores del Dominio y de los Activos. Como no por ser imprecisa es menos delicada, requiere una colaboración estrecha de los dos profesionales implicados, el Responsable del Dominio protegible por una parte y el Analista de Riesgos por otra.
Esta propiedad se termina por expresar con un valor decimal, comprendido entre los valores extremos 0 (la Amenaza no afecta al Activo) y 1 (no alcanzable pues significa la agresión permanente). Sin entrar en justificaciones teóricas que corresponden más a éste que a aquél, se debe hace constar que MAGERIT evita cuidadosamente los términos ***probable*** y ***probabilidad*** al definir la Vulnerabilidad, mientras que emplea los conceptos de ***potencial*** y ***potencialidad*** como más cercanos al tránsito de amenaza materialiable en agresión. Esa potencialidad se convierte en ***frecuencia*** para los casos de calculabilidad definida (por ejemplo cuando el fabricante da la cifra de cuántas veces falla una disquetera por año) y en ***posibilidad*** para los casos de calculabilidad más difusa (que MAGERIT también trata con técnicas avanzadas especiales).

Cuando se realiza la estimación de Vulnerabilidad de los Activos no se parte de cero y conviene precisar bien el contexto de realización de la estimación, ya que al menos pueden observarse dos valores de vulnerabilidad distintos.

Por una parte, la creciente madurez y calidad de las Tecnologías de la Información y la Comunicación es difícil que no haya incorporado a todo Activo relacionado con ellas muchas salvaguardas de protección contra las amenazas técnicas más frecuentes; por tanto la estimación de la vulnerabilidad debe siempre referirse a un estado dado de la tecnología que dé por implícitas dichas protecciones y partir de dicho estado como base de cálculo de la **vulnerabilidad intrínseca** para cada amenaza pertinente. Éste es el tipo de vulnerabilidad para cuya estimación se requiere mayormente la contribución del Responsable del Dominio protegible.

Por otra parte, la mayoría de proyectos de seguridad se refieren a un Dominio existente en los que su Responsable ya ha implantado mecanismos de salvaguarda. La **Vulnerabilidad efectiva** del Activo respecto a una Amenaza concreta tiene en cuenta esos mecanismos de salvaguarda como un factor que estima su ***eficacia*** global. El Análisis y Gestión de Riesgos suplementa esos mecanismos si es necesario o bien los sustituye si fuera conveniente e incluso los reduce si resultan ineficaces o contraproducentes. La estimación de este tipo de vulnerabilidad es más complicada y reposa más en el analista de riesgos.

MAGERIT mide la Vulnerabilidad por la ***frecuencia*** histórica cuantitativa de la materialización de la Amenaza sobre el Activo, cuando es factible (fiabilidad de un componente hardware, número de fallos de software...); o bien por la ***potencialidad*** cualitativa de dicha materialización, cuya primera aproximación lleva a emplear una escala vista en las Amenazas potenciales (consideradas ahora reales, o sea agresiones). En este caso, el Responsable del Dominio protegible es quien puede dar, con su experiencia concreta de manejo de los Activos a su cargo, una apreciación suficiente del nivel de Vulnerabilidad a partir de una escala de 'pseudo-frecuencias' como la siguiente para el caso habitual de los Sistemas de Información para la Gestión (otros sistemas con objetivos distintos pueden requerir otras escalas, que el Analista de Riesgos adaptaría en cada caso).

Periodo medio entre ocurrencias	**Escala subjetiva**
menor de 1 semana	Frecuencia muy alta
menor de 2 meses	Frecuencia alta
menor de 1 año	Frecuencia media
menor de 6 años	Frecuencia baja

superior a 6 años	Frecuencia muy baja

Si el analista cree que conviene un análisis muy detallado de la **Vulnerabilidad intrínseca** citada, el Responsable del Dominio protegible puede ayudarle en la estimación de ésta. Por ejemplo, una

Amenaza de 'inundación por desbordamiento de torrente' relativa a un Activo 'centro de cálculo' se plasma en una Vulnerabilidad del Activo ante esa Amenaza. La Vulnerabilidad depende tanto del 'ciclo de recurrencia' (frecuencia) de las inundaciones en la zona como de la ubicación del propio centro de cálculo (cercanía al lecho, situación en un sótano, etc.). Los dos componentes básicos de la vulnerabilidad intrínseca son:

- **Potencialidad autónoma** respecto al Activo amenazado de la ocurrencia de la Amenaza (por ejemplo la frecuencia de inundaciones en un lugar determinado).

- **Potencialidad derivada** de la relación entre Activo y Amenaza, sobre todo si es **intencional**, que en este caso puede descomponerse en:

  **** Factores subjetivos*** generadores por ejemplo de más o menos motivación.

  **** Oportunidad de acceso*** al Dominio de un agresor con suficientes recursos, como:

  - ***Accesibilidad física presencial:*** número de personas o entidades autorizadas por su función a acceder normalmente al entorno del Activo, con una escala que va de accesibilidad muy alta (bastantes personas de varios entidades distintas) a muy baja (una persona o entidad).

  - ***Accesibilidad física calificada:*** calificación (formación general y experiencia) de los usuarios autorizados a acceder físicamente al entorno del Activo, con una escala que va de accesibilidad muy alta (no se requiere calificación) a muy baja (requiere gran formación y experiencia para manejar la documentación técnica).

  – ***Accesibilidad lógica competencial.*** Conocimiento técnico específico sobre el Activo atacable, con una escala que va de accesibilidad muy alta (no requiere competencia especial) a muy baja (necesita un experto muy calificado).

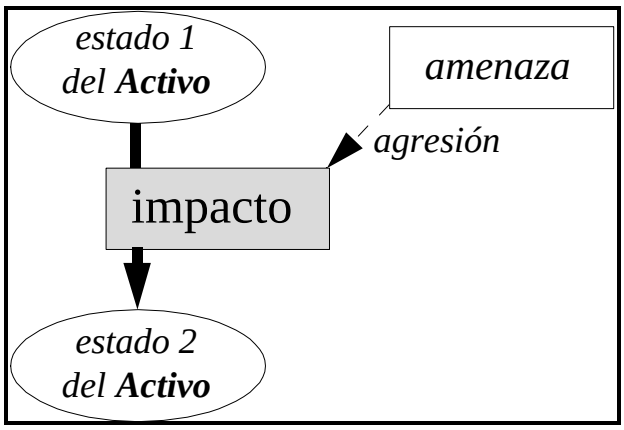
  - ***Accesibilidad lógica instrumental.*** Disponibilidad del instrumental que corresponde a la tecnología del Activo amenazable, con una escala que va de accesibilidad muy alta (no requiere instrumental o éste es muy accesible) a muy baja (requiere instrumental especial y de acceso muy difícil).

El Analista de Riesgos (con ayuda de la herramienta que emplee) convertirá en factores correctores de la ***Potencialidad autónoma*** los factores subjetivos anteriores y los niveles de los tipos de accesibilidad

que le proporcione el Responsable del Dominio protegible

2.5 Identificación de Impactos

El Impacto en un Activo es la consecuencia sobre éste de la materialización de una Amenaza en agresión, consecuencia que puede desbordar ampliamente el Dominio y requerir la **medida** del **daño** producido a la organización. Visto de forma más dinámica, Impacto es la diferencia en las estimaciones del **estado** (de seguridad) del Activo obtenidas antes y después del evento de agresión.



El Responsable del Dominio protegible para realizar la estimación crucial de los Impactos se apoya en la tipología de Impactos de MAGERIT, orientada a la ***naturaleza de las Consecuencias*** de las combinaciones Activo-Amenaza. Siguiendo esta orientación, no constituiría normalmente un Impacto, si no entraña una Consecuencia de deterioro y perjuicio apreciable como cambio de estado del Activo, una simple disfunción de éste, como por ejemplo la interrupción del tratamiento de una aplicación en un sistema por microcorte de energía o el reenvío automático de un mensaje por un servicio que tenga mecanismos de auto-recuperación (aunque estas disfunciones impliquen incluso formas más o menos degradadas de funcionamiento, pues normalmente ya se cuenta con ellas).

MAGERIT considera tres grandes grupos de Impactos, según que sus ***Consecuencias*** sean ***reductoras*** del ***estado*** de seguridad del Activo agredido ***directamente*** (en este caso el Impacto se compone de su Gravedad intrínseca y un Agravante o Atenuante circunstancial); o ***indirectamente*** (y en este caso, de forma ***cualitativa*** o ***cuantitativa***). Entonces el Impacto será:

- **cualitativo con pérdidas funcionales** (de los subestados de seguridad) del Activo
- o bien **cualitativo con pérdidas orgánicas** (de fondo de comercio, daño de personas,..)
- o bien **cuantitativo** si las consecuencias se puede traducir a dinero.

Ciertos Impactos suponen consecuencias cualitativas funcionales sobre los subestados:

- El **Subestado de Autenticación SA** se define como la característica de dar y reconocer la identidad y autorización de las personas respecto a Activos del Dominio (de tipo ***Información)*** y está ligado a requerimientos de ***formalización o responsabilización probatoria*** del conocimiento o de la comunicación de esos Activos (para conseguir su eficacia jurídica si es información manejada por las Administraciones Públicas en un Estado de derecho, o bien su calidad contractual en las transacciones financieras del llamado comercio electrónico en el sector privado). Aunque el deterioro del subestado de autenticación no suele 'multiplicarse en cadena', puede producir la anulación de documentos y procedimientos e indirectamente inseguridad jurídica (de ahí su importancia sobre todo en la Administración pública). Para entender los niveles de autenticación, se puede usar el ejemplo de un mensaje-carta de correo tradicional. El nivel del estado de autenticación de este Activo se considera ***bajo*** si se trata de información que como mucho requiere saber si hubo acceso a ella (el sobre llega abierto); ***medio*** si además se requiere 'sobre certificado' para que no se pueda 'negar' o repudiar su origen o su destino; ***alto*** se además se requiere certificación con acuse de recibo para que no se pueda negar su destino; y ***muy alto*** si además se requiere certificación del 'autor' y del contenido (con mecanismos de firma electrónica y reconocimiento por tercera parte de confianza).

- El **Subestado de Confidencialidad SC** se define como la característica opuesta al conocimiento por personas no autorizadas de Activos del Dominio (de tipo ***Información*** sobre todo). Se relaciona con la intimidad cuando la Información se refiere a personas físicas, tratada por la LORTAD, Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de carácter personal; pero también concierne a activos como manuales de usuario o desarrollo, aplicaciones informáticas, etc. El deterioro de la Confidencialidad tampoco suele 'multiplicarse', pero su reducción en la escala de niveles (muy alta, alta, media, baja) tiene consecuencias directas (divulgación de información no revelable o bien revelada anticipadamente, sustracción puntual o masiva) o indirectas (desconfianza, incomodidades, chantaje...).

- El **Subestado de Integridad SI** se define como la característica opuesta a la modificación o destrucción no autorizadas de Activos del Dominio. La integridad está vinculada a la ***fiabilidad funcional*** del sistema de información (o sea su eficacia para cumplir las funciones del sistema de organización soportado por aquél) y suele referirse (no siempre) a Activos de tipo ***Información o*** **sistema de información** en el caso del software y su respectiva documentación. Por ejemplo, son típicos los problemas causados por la amenaza de un virus (llegado con un disquete externo o por la red) a la integridad de los datos almacenados en el disco duro de un PC. El deterioro de la ***Integridad si que puede multiplicarse en cadena*** y tiene consecuencias directas (como la alteración de información sensible o vital en mayor o menor escala) e indirectas (como la posible contaminación de programas con pérdida, tratamiento erróneo, etc.). Los **niveles** referidos a la ***necesidad*** de integridad suelen referirse a la facilidad y coste mayor o menor de reproducir Activos de igual calidad a los deteriorados.

- El **Subestado de Disponibilidad SD** se define como la posibilidad de acceder o usar el Dominio por las personas autorizadas. La disponibilidad se asocia a la ***fiabilidad técnica*** (tasa de fallos) de los componentes del sistema de información. El deterioro de la Disponibilidad **sí** que puede multiplicarse en cadena y tener consecuencias directas tanto inmediatas como duraderas (desde la degradación de la productividad del activo como recurso hasta la interrupción de su funcionamiento de forma más o menos profunda de unos datos, de una aplicación, de un servicio o de todo un sistema). Indirectamente esto se traduce en caída de margen por falta de resultados; y en gastos suplementarios para recuperar o mantener la funcionalidad precedente a la amenaza. Sus niveles se estructuran en una escala definida por el período de **tiempo máximo de carencia** del Activo. MAGERIT usa esta **escala** simple, válida para sistemas de información normales en los sectores público y privado, que se usa con mucha frecuencia para apreciar globalmente el Impacto (como se detalla después):

  - menos de una hora
  - menos de un día laborable
  - menos de una semana
  - menos de un mes
  - más de un mes

Una parte de estos deterioros de los subestados de seguridad tienen Impactos con consecuencias cuantitativas de varios tipos:

- ***N1: Pérdidas de valor económico, ligadas a activos inmobiliarios o inventariables,*** que comprenden todos los costes de reposición de la funcionalidad, incluyendo los gastos de tasar, sustituir, reparar o limpiar lo dañado: edificios y obras, instalaciones, computadores, redes, accesorios, etc..
- ***N2: Pérdidas indirectas, valorables y ligadas a intangibles en general no inventariados:*** gastos de tasación y restauración o reposición de elementos no materiales del sistema: datos, programas, documentación***,*** procedimientos, etc.
- ***N3: Pérdidas indirectas,*** valorables ***económicamente,*** unidas a ***disfuncionalidades tangibles:*** se aprecian por el coste del retraso o interrupción de funciones operacionales de la organización; la perturbación o ruptura de los flujos y ciclos productivos (de productos, servicios o expedientes, por ejemplo), incluido el deterioro de la calidad de éstos; y la incapacidad de cumplimentar las obligaciones contractuales o estatutarias .

- ***N4: Pérdidas económicas relativas a responsabilidad legal*** del 'propietario' del Dominio protegible siniestrado debido a los perjuicios causados a terceros (incluidas por ejemplo multas de la A**gencia de Protección de Datos).**

Otros deterioros de los subestados de seguridad tienen Impactos con consecuencias cualitativas orgánicas de varios tipos:

- ***L1: Pérdida de fondos patrimoniales intangibles:*** conocimientos (documentos, datos o programas) no recuperables, información confidencial, 'know-how' ...

- ***L2: Responsabilidad penal por Incumplimiento de obligaciones legales*** (Ley Orgánica 5/1992 LORTAD, Ley 30/1992 LRJPAC)

- ***L3: Perturbación o situación embarazosa político-administrativa*** (deontología,credibilidad, prestigio, competencia política ...)

- ***L4: Daño a las personas***

2.6 Estimación de Impactos

La cuantificación de los Impactos es no sólo uno de los procesos más difíciles del Análisis de Riesgos, sino que es el más influyente en el cálculo del propio Riesgo. Como se verá en el Modelo de Eventos, el nivel del Riesgo depende directamente de la Vulnerabilidad y del Impacto, pero se da a éste un peso mayor por todo el mundo en el proceso de decisión que subyace al cálculo del riesgo.

MAGERIT indica varias formas de valorar estos impactos:

- valoración económica directa de las ***Pérdidas Cuantitativas N*** cuando es posible. (La única que es cuantitativa)

- Estimación por niveles usando **una escala monetaria** meramente orientativa que representa las cantidades a emplear para paliar los daños producidos por una amenaza materializada en la organización.

Rango de valores (en pesetas)	***Impacto***
– menor que 100.000	Muy bajo
– menor que 1.000.000	Bajo
– menor que 10.000.000	Medio
– menor que 100.000.000	Alto
– mayor que 100.000.000	Muy Alto

- Estimación por **Niveles de Gravedad** usando las escalas cualitativas de las Pérdidas cualitativas L orgánicas o de las funcionales relacionadas con reducción de los subestados SA de Autenticación, SC de Confidencialidad o SI de Integridad. Esta Gravedad puede requerir la apreciación de **Agravantes** (o Atenuantes) circunstanciales distintos para los cuatro subestados.

- Valoración en tiempo de la falta de **disponibilidad** de algún activo importante, teniendo en cuenta como atenuantes la redundancia o la multifuncionalidad de los Activos amenazables.

Aunque la finalidad de MAGERIT es medir los impactos en pesetas u otros índices objetivos semejantes, esto no siempre resulta posible, salvo si se usan métodos ***indirectos*** y a menudo inadecuadamente ***subjetivos***. Por tanto el Responsable del Dominio protegible sigue el siguiente proceso, en colaboración con el Analista de Riesgos:

- en un primer intento intenta escoger como medida del impacto el coste de reposición del activo dañado;
- cuando esta medida no es factible o no tiene sentido, intenta apreciar el coste de reposición de la función realizada por el Activo dañado, a partir del deterioro de alguno de sus subestados de seguridad. Así:
  - La pérdida con gravedad alta del subestado de ***disponibilidad*** de un Activo de tipo información (reponible con gran dificultad) afecta total o parcialmente a una funcionalidad de la Organización durante un tiempo determinado (por ejemplo, si se pierde la información sobre los Pedidos, se pierde un mes de facturación).
  - La misma pérdida con gravedad alta del subestado de ***confidencialidad*** no hace perder facturación actual, pero puede haber dado la lista de pedidos a un competidor que la usará para hacer perder clientes y su facturación futura; pérdida posiblemente mucho más alta, si no se toman las medidas adecuadas en el intervalo.

2.7 Riesgo

El riesgo es la **posibilidad** de que se produzca un **impacto** en un Activo o en el Dominio.
Para MAGERIT el cálculo del riesgo ofrece un **Indicador** que permite **tomar decisiones** por comparación explícita con un **Umbral de Riesgo** determinado; o sea una propiedad de la relación Vulnerabilidad /Impacto y por tanto de la relación entre Activos y Amenazas.
El Responsable del Dominio protegible ayuda a establecer los umbrales de riesgo como parte de su estrategia de seguridad en su Dominio, a partir de los cálculos de los distintos riesgos que realiza el Analista de Riesgos.

2.8 Mecanismos de salvaguarda

Una **Función** o un **Servicio** de salvaguarda es una acción genérica que reduce el Riesgo mientras que

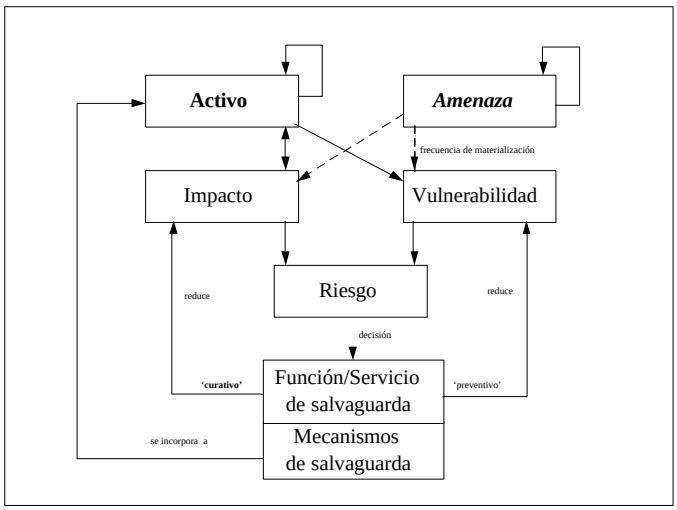
un **Mecanismo de salvaguarda** es el procedimiento o dispositivo, físico o lógico, capaz de reducir el riesgo. Actúa de dos formas posibles, en general alternativas:

- neutralizando o bloqueando la ***materialización de la Amenaza*** antes de ser agresión
- mejorando el ***estado de seguridad*** del Activo ya agredido, por reducción del Impacto.

Los **mecanismos de salvaguarda** se valoran directamente por su coste técnico u organizativo, traducidos a pesetas.

2.9 Interrelación entre los elementos de seguridad

El esquema de relaciones entre elementos del Modelo de Seguridad de MAGERIT que se ha presentado puede ayudar a comprender el funcionamiento del método y a resumirlo (las flechas 'reentrantes' de los Activos y Amenazas representan relaciones entre sí, es decir 'cadenas').

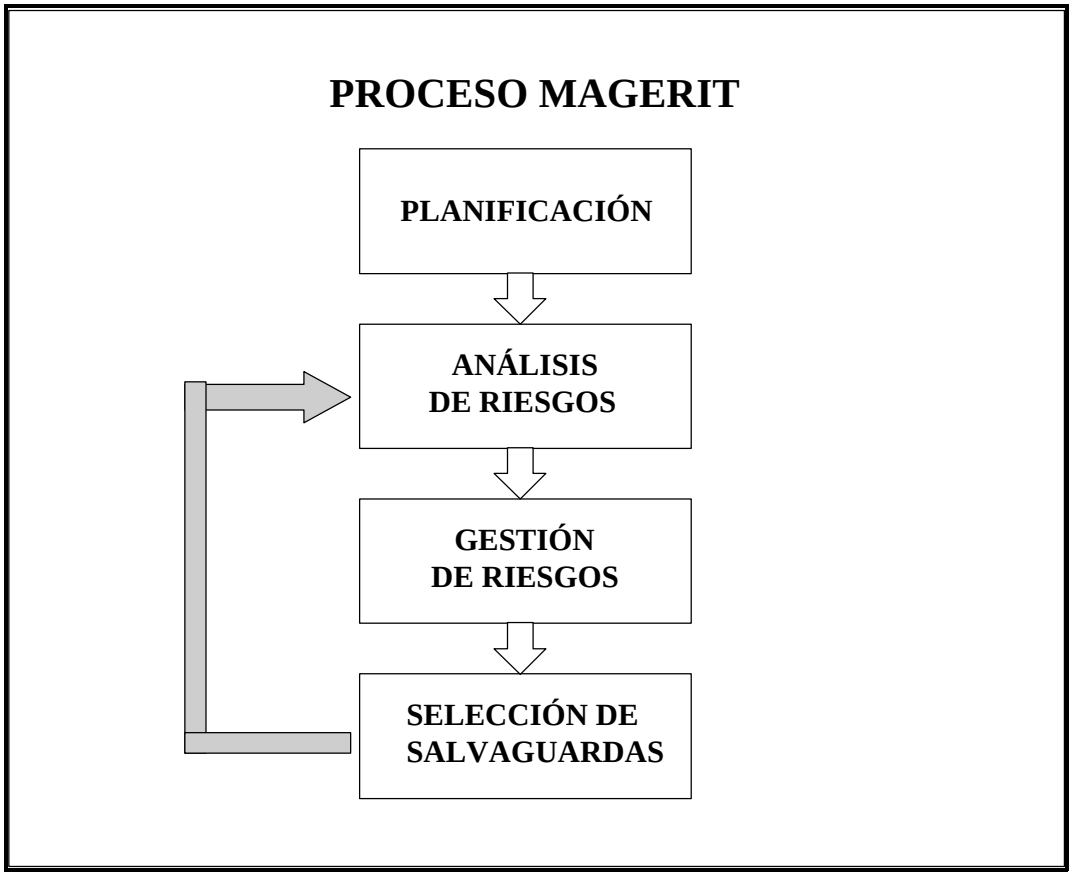


3. PARTICIPACIÓN DEL RESPONSABLE DEL DOMINIO EN MAGERIT

El Responsable del Dominio protegible participa en varias etapas de MAGERIT, bajo la orientación del Analista de Riesgos.

3.1 Descripción breve de las etapas del proceso que sigue MAGERIT

El proceso de MAGERIT consta de estas cuatro Etapas:



En la Etapa 1 de **Planificación** del Análisis y Gestión de Riesgos se establecen las consideraciones necesarias para arrancar el proyecto, investigando la oportunidad de realizarlo, definiendo los objetivos que ha de cumplir y el dominio (ámbito) que abarcará, planificando los medios materiales y humanos para su realización e iniciando materialmente el propio lanzamiento del proyecto

En la Etapa **2** de **Análisis de riesgos** se identifican y valoran los diversos elementos componentes del riesgo, obteniendo una estimación de los umbrales de riesgo deseables.

En la Etapa **3** de **Gestión de riesgos** se identifican las posibles **funciones** y **servicios** de salvaguarda reductores del riesgo calculado, se seleccionan los aceptables en función de las existentes y otras restricciones y se especifican los elegidos finalmente.

En la Etapa **4** de **Selección de salvaguardas** se escogen los mecanismos de salvaguarda a implantar, se elabora una orientación de ese plan de implantación, se establecen los procedimientos de seguimiento para la implantación y se recopila la información necesaria para obtener los productos finales del proyecto y realizar las presentaciones de resultados.

Cada una de esta Etapas se subdividen en 19 Actividades, y éstas en Tareas que se detallan en la Guía de Procedimientos.

3.2 Intervención del Responsable del Dominio

El **Responsable del Dominio protegible** además de recibir información de los resultados finales de las Etapas, interviene básicamente en las tres Actividades siguientes: (entre las 19 Actividades que forman el Submodelo de procesos de MAGERIT).

3.2.1 Intervención en la Actividad 1 de la Etapa 2: 'Recogida de información'

En esta actividad el Analista de Riesgos recoge la información sobre el sistema y de los factores que pueden influir en la seguridad por medio de entrevistas concertadas a los **Responsables de los distintos**

Dominios protegibles estudiados.

El Analista de Riesgos comienza la Preparación de la Recogida de Información con acciones encaminadas a:

- Recopilar los cuestionarios personalizados en la etapa anterior
- Ubicar y localizar a los entrevistados, para optimizar la realización de las entrevistas
- Confirmar las entrevistas
- Recordar los objetivos de la entrevista al entrevistado
- Informar de los documentos requeridos en la entrevista, para facilitar su disponibilidad
- Disponer de documento acreditativo de la Dirección, que muestre su apoyo al proyecto.

Durante la entrevista el Analista profundiza con el Responsable del Dominio protegible:

- Definición de las funciones y objetivos del entrevistado
- Descripción del modo de actuación
- Identificación de los procesos realizados y los datos manejados
- Medios disponibles para realizar las funciones y del personal del Dominio
- Descripción del entorno
- Identificación de posibles situaciones conflictivas relacionadas con la seguridad.

3.2.2 Intervención en la Actividad 1 de la Etapa 3: 'Interpretación del riesgo'

El Analista de Riesgos tras interpretar los riesgos calculados para detectar las áreas críticas, consulta al Responsable del Dominio protegible los niveles de riesgos de sus áreas, proponiendo una primera estimación del umbral de riesgos y del riesgo residual.

3.2.3 Intervención en la Actividad 2 de la Etapa 4: 'Selección de mecanismos'

El Analista de Riesgos selecciona los **mecanismos de salvaguarda** que materialicen las funciones y servicios de salvaguarda, respetando las restricciones del **Responsable del Dominio protegible** al que consulta el nivel de riesgo residual tras aplicar mecanismos.

4 FUNCIÓN DEL RESPONSABLE DEL DOMINIO

En definitiva, el Responsable del Dominio protegible, por su profundo conocimiento de éste, tiene como misión principal cooperar con el Analista de riesgos en identificar y valorar los elementos del Análisis y Gestión de Riesgos, en particular:

- la identificación de los Activos, así como su valoración
- la estimación de los subestados de la seguridad (autenticación, confidencialidad, integridad y disponibilidad)
- la interdependencia de los diversos activos para cumplir su misión
- la detección de las amenazas que puedan atacar a los activos
- la clarificación de los factores que pueden incrementar la vulnerabilidad
- la magnitud que un impacto provoca sobre un activo al materializarse una amenaza
- el establecimiento de un umbral aceptable de Riesgo para los activos
- la especificación de los Mecanismos de salvaguarda ya implantados en el dominio
- la consulta de los Mecanismos de salvaguarda que recomienda el Analista de Riesgos.

5. CUADRO RESUMEN

Esta Guía parte de una constatación esencial. El **Responsable del Dominio Protegible** es el mejor conocedor de las funciones de su Dominio y de su importancia, del Sistema de Información utilizado y del entorno de éstos. Por tanto es quien puede aportar la valiosa información que permitirá al Analista de Riesgos calcular los riesgos y proponer las salvaguardas que protegerán el cumplimiento de la misión o cometido del Responsable de Activos Protegibles.

El **Responsable del Dominio Protegible** colabora con el Analista de Riesgos en múltiples funciones de gran importancia para lograr el éxito del proyecto:

0. identifica activamente tres aspectos principales:

   - El conjunto de los Activos y su entorno correspondientes a su dominio
   - La interrelación de los Activos para construir árboles de activos
   - El grado de dependencia entre los Activos de cada árbol

1. valora decisivamente los activos cuantitativamente por su valor de cambio (cuando es posible) y cualitativamente por su valor de uso.
2. interviene en la detección de las posibles amenazas sobre los activos.
3. ayuda intensamente en la evaluación de los factores que conforman la vulnerabilidad.
4. ejerce un papel fundamental en la identificación de los impactos que la materialización de una amenaza podría causar sobre los activos
5. ejerce un papel fundamental en la estimación de los impactos que la materialización de una amenaza podría causar sobre los activos
6. ayuda a validar el establecimiento de umbrales de riesgos considerados como óptimos
7. colabora en la identificación de los mecanismos de salvaguarda ya implantados en el Dominio y en la aprobación de los demás mecanismos idóneos para rebajar los riesgos a los umbrales establecidos

Asimismo, el Responsable del Dominio protegible interviene junto al Analista en tres Actividades precisas del procedimiento de desarrollo de MAGERIT:

1. En la Recogida inicial de información (Etapa 2 Actividad 1)
2. En la Interpretación del riesgo (Etapa 3 Actividad 1)
3. En la Selección final de mecanismos de salvaguarda (Etapa 4 Actividad 2)

ANEXO 1: EQUIPO RESPONSABLE DEL PROYECTO

Coordinador del Proyecto:
D. Víctor M. Izquierdo Loyola
Subdirector General de Coordinación Informática - MAP

Director del Proyecto:
D. Francisco López Crespo
Jefe de Área de Asistencia Técnica- MAP

Secretario del Proyecto:
D. Miguel A. Amutio Gómez
Técnico Superior de Tecnologías de la Información - MAP

Grupo de Expertos

Dña.Mª Dolores Hernández Maroto MINISTERIO DE ADMINISTRACIONES PÚBLICAS	D. Carlos García Codina MINISTERIO DE SANIDAD Y CONSUMO
D. Andrés Barreiro Pérez MINISTERIO DE ECONOMÍA Y HACIENDA	D. Arturo Ribagorda Garnacho UNIVERSIDAD CARLOS III
D. Carlos López Martín MINISTERIO DE DEFENSA	D. Cecilio Salmerón Giménez BANCO DE ESPAÑA
D. Emilio Lorenzo Gil ORGANISMO AUTÓNOMO CORREOS Y TELÉGRAFOS	Dª Rosa Mª García Ontoso INFORMÁTICA DE LA COMUNIDAD DE MADRID
Dª Clara Cala Rivero MINISTERIO DE INDUSTRIA Y ENERGÍA	

Empresa consultora externa

SEMA GROUP
Director de proyecto: Julián Marcelo Cocho
Consultor Principal: Santiago Martin-Romo Romero